AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
(A) 11 Genesee Street, Apartment 1, Greene, NY 13778, (B) the person of Brock Likens; (C) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data/media,further described in Attachment B

Case No. 3:18-mj-36(ATB)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):* (A) 11 Genesee Street, Apt. 1, Greene, NY 13778; (B) the person of Brock Likens; (C) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data/media, further described in Attachment B

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized):*
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252 and 2252A	Transporting, Receiving, Distributing or Possessing Child Pornography

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jenelle Bringuel, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/23/2018

Judge's signature

City and state: Syracuse, New York

Hon. Andrew T. Baxter, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR SEARCH WARRANT FOR:

[SEE ATTACHMENT A, HEREIN]

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

JENELLE CORRINE BRINGUEL, being duly sworn, deposes and states:

INTRODUCTION

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I am investigating the activities of the IP address 198.255.143.203, subscribed to by Geri Hewitt, who resides at 11 Genesee Street, Apartment 1, Greene, NY 13778 (the Subject Premises, as more fully described in Attachment A). As will be shown below, there is probable cause to believe that someone using the IP address registered to Geri Hewitt at the Subject Premises has transported, received, possessed, or distributed child pornography, in violation of 18 U.S.C.§§ 2252 and 2252A, and I submit

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR SEARCH WARRANT FOR:

[SEE ATTACHMENT A, HEREIN]

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

JENELLE CORRINE BRINGUEL, being duly sworn, deposes and states:

INTRODUCTION

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.

3. I am investigating the activities of the IP address 198.255.143.203, subscribed to by Geri Hewitt, who resides at 11 Genesee Street, Apartment 1, Greene, NY 13778 (the Subject Premises, as more fully described in Attachment A). As will be shown below, there is probable cause to believe that someone using the IP address registered to Geri Hewitt at the Subject Premises has transported, received, possessed, or distributed child pornography, in violation of 18 U.S.C.§§ 2252 and 2252A, and I submit

this application and affidavit in support of a search warrant authorizing a search of (A) 11 Genesee Street, Apartment 1, Greene, NY 13778, (B) the person of Brock Likens and (C) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches. Located within the places and items to be searched, I seek to seize evidence, fruits, and instrumentalities of criminal violations relating to the knowing transportation, shipment, receipt, possession, and distribution, of child pornography, as more particularly described in Attachment B.

4. As will be demonstrated in this affidavit, made under Fed. R. Crim. P. Rule 41, there is probable cause to believe that evidence will be located at the Subject Premises, on the person of Brock Likens, and within computers, computer equipment and/or other electronic media relating to violations of Title 18, United States Code 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography), hereafter referred to as the Subject Offenses.

5. The statements and facts set forth in this affidavit are based in significant part on: my review of written documents obtained from the FBI Albany Child Exploitation Task Force, my conversations with Village of Greene Police Department Officer Jeff Messina, and my personal training and experiences. Since this Affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Sections 2252 and 2252A are presently located within the places and items to be searched.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

6. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, I know that electronic devices, including computers and cellular telephones serve different roles or functions with child pornography: production, communication, distribution, and storage.

7. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within recent years. These drives can store thousands of images at very high resolution.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

11. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In

addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

PEER TO PEER FILE SHARING

12. Millions of computer users throughout the world use Peer-To-Peer (P2P) file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

13. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. Often, however, a user downloading a file receives the entire file from one computer.

14. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

15. P2P software users can search the P2P network by entering search terms into their P2P software to generate a list of available files that contain the search terms. For example, a person interested

in obtaining child pornographic images would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user then selects from the results the file(s) he/she wants to download. The files are downloaded directly from the computer sharing the file. The downloaded files are stored in the area or directory previously designated by the user and/or the software. The downloaded files will remain in that same location until moved or deleted.

16. Law Enforcement can search the P2P networks to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. When a user on the P2P network offers a file to trade, the P2P software used by law enforcement calculates a "hash value" of the file using a SHA-1 hash. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology, along with the National Security Agency, as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. A hash is a mathematical function that converts the data that comprises the contents of a file into an alphanumeric value. This value is unique to every file. A person may copy a file and rename it but if it is an exact copy, regardless of the name of the file, it will have the same hash value.

17. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. By comparing these hash values, one can determine whether two files are identical with a precision that greatly exceeds 99.9999 percent certainty.

18. An investigator can examine the SHA-1 hash values of files being traded on the P2P network and determine if they are the same as the hash value of a file known to be child pornography. The investigator is able to do this by comparing the hash value associated with a file offered on the P2P network with hash values of movies or images of child pornography identified from previous investigations. The use of SHA-1 hash values for the matching of movies and images has proven to be

extremely reliable. The investigator can then verify the contents of the file by viewing a copy of the file that has the same hash value from a library of known and/or suspected child pornography files kept by the investigator.

19. Most P2P programs allow users to designate specific folder(s) as "shared" folders. Any files contained in those specific folders are then made available for download by other users on the same P2P network. P2P software users typically do not "share" all of the files on their hard drive.

20. The BitTorrent network is a very popular and publically available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients," hereafter referred to as a peer. A peer can download files from other peers simultaneously, and provide these files to other peers.

20. The BitTorrent network can be accessed by computers via many different client (software) programs, such as the "BitTorrent" program, the "µTorrent" program, the "BitLord" program, and the "Vuze" program, to name a few. These client programs are publicly available, typically free, and can be downloaded from the Internet.

21. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between an investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

COLLECTORS OF CHILD PORNOGRAPHY

22. Individuals who are interested in child pornography may want to keep the child pornography files they receive for use in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy and security of their homes or other secure location. Additionally,

individuals who utilize social media are known to keep their electronic media with them, including at their homes.

23. Individuals who collect child pornography may seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, mail, email groups, bulletin boards, IRC, newsgroups, instant messaging, Peer to peer programs, and other similar vehicles.

24. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.

25. Individuals who collect child pornography may keep names, e-mail addresses, phone numbers or lists of persons who have shared, advertised or otherwise made known their interest in child pornography or sexual activity with children. These contacts may be maintained as a means of personal referral, exchange or commercial profit. This information may be maintained in the original medium from which it was derived, in lists, telephone or address, on computer storage devices, or merely on paper.

BACKGROUND OF THE INVESTIGATION

26. On Saturday, November 18th, 2017, Christopher Smith, a Colonie Police Department Police Officer, and member of the FBI's Albany Child Exploitation Task Force, accessed the Internet while acting in a covert capacity, and conducted an investigation into the sharing of child pornography files on a BitTorrent P2P file-sharing network. On November 18, 2017, Smith completed

the download of 1 file that the device at IP 198.255.143.203 was making available to share on the BitTorrent network. The device at IP address 198.255.143.203 was the sole candidate for each download, and as such, that file was downloaded directly from this IP address. The IP address was recorded, along with the date, time, and hash value of the file transfer.

27. On November 19, 2017, Smith completed the download of 38 files that the device at IP 198.255.143.203 was making available to share on the BitTorrent network. The device at IP address 198.255.143.203 was the sole candidate for each download, and as such, that file was downloaded directly from this IP address. The IP address was recorded, along with the date, time, and hash value of the file transfer.

28. On November 26, 2017, Smith completed the download of 48 files that the device at IP 198.255.143.203 was making available to share on the BitTorrent network. The device at IP address 198.255.143.203 was the sole candidate for each download, and as such, that file was downloaded directly from this IP address. The IP address was recorded, along with the date, time, and hash value of the file transfer.

29. The downloaded files were provided to and reviewed by your Affiant. Eighty-seven (87) complete video files and nine (9) partial video files were downloaded between November 18 and 26, 2017. All of the complete videos (87) and seven (7) of the partial videos depict child pornography. Two of the partial video files were unable to be opened; however, the file names are indicative of child pornography and are similar to other downloaded file names. The downloaded files are available for the court's review upon request, and three of them are described as follows:

a. On 11/18/2017, a file bearing the name "Babyj & Babyshivid 2Yo.avi" was downloaded from a device utilizing IP address 198.255.143.203. This video, approximately 39 seconds in length depict a nude child, approximately 2 years of age, standing in front of an ottoman with their back facing the camera and their hands tied behind their back. An adult male penis can be seen behind the child. The adult male squirts a white substance on the rear end of the child and

massages it into their rear end. The adult male then picks the screaming child up and bends them over the ottoman.

b. On 11/19/2017, a file bearing the name "Babyshivid-pussy-01.avi" was downloaded from a device utilizing IP address 198.255.143.203. This video, approximately 1 minute in length depicts a female child approximately 2 years of age, laying on her back wearing only a pair of underwear and a blindfold. A nude adult male is standing over the child forcing her legs back toward her head. The adult male moves the crotch of the child's underwear to the side and rubs his penis against her vagina. After several attempts at inserting his penis into the child's vagina, the adult male vaginally penetrates the crying child with his penis.

c. On 11/26/2017, a file bearing the name "Babyshivid-pussy-pounded.avi" was downloaded from a device utilizing IP address 198.255.143.203. This video, approximately 2 minutes and 44 seconds in length depicts a nude female child approximately 2 years of age, laying on her back while a nude adult male kneels above her with his buttocks over her head area. The adult male rubs his penis over the child's vaginal area. After several attempts at inserting his penis into the child's vagina, the adult male vaginally penetrates the child with his penis and eventually ejaculates on her vaginal area.

30. A search of the American Registry for Internet Numbers (ARIN) online database for IP address 198.255.143.203 revealed that the IP address belongs to Time Warner Cable. The results of an administrative subpoena that was sent to Time Warner cable on 1/9/2018 revealed that the aforementioned IP address was assigned to subscriber Geri Hewitt, 11 Genesee Street, Apartment 1, Greene, NY 13778 between 6/8/2017 and 12/3/2017, which encompasses the dates Smith completed the downloads of child pornography files from IP address 198.255.143.203.

31. During physical surveillance conducted on January 12, 2018, it was determined that all wi-fi networks located at and around the Subject Premises, available at the time, were secured.

32. On January 12, 2018, your Affiant met with the Village of Greene (Greene, NY) Police Officer Jeffrey Messina, who provided your Affiant with a list of the utility subscribers for the apartments at 11 Genesee Street, Greene, NY 13778. The current utility subscriber for the Subject Premises is Geraldine Hewitt. Officer Messina is familiar with the Subject Premises and the occupants, as he conducted an interview on an apparently unrelated matter of Hewitt's grandson, Brock Likens, at that residence approximately a year ago.

33. After speaking to your Affiant, on January 12, 2018, Officer Messina knocked on the door of the Subject Premises. Prior to knocking, Officer Messina told your Affiant he heard what sounded like children's voices on a television or computer inside the apartment. Upon knocking, Officer Messina could tell the volume was turned down on whatever the voices had been emanating from. A male by the name of Brock Likens answered the door and Officer Messina recognized him as the grandson of Geraldine Hewitt whom he had interviewed at that same residence the previous year. Likens initially appeared very nervous and was wringing his hands. Officer Messina could see into the interior of the apartment and all of the windows were blacked out with curtains. Likens told Officer Messina that he lived in the apartment with his grandmother, Geraldine Hewitt.

34. On January 18, 2018, the United States Postal Service provided to your Affiant information confirming that the individuals receiving mail at the Subject Premises are Geraldine Hewitt and Brock Likens.

35. The apartment building of 11 Genesee Street, Greene, NY 13778 is a two-story light grey home with a white front porch, situated on the south side of Genesee Street. The front exterior doors and trim around the windows are white. There are four grey steps leading up to the porch in the front of the residence. On the first level, the front doors are situated in the middle of the home, and there is a window situated to each side of the front doors. On the second level of the house, there are five windows across the front of the home. In what appears to be the attic of the residence, there is a window positioned on the front of the house, in the middle, directly above the front doors and a window on the second floor of the home. Apartment 1 is situated inside the left front door on the left side of the residence. The mailboxes

for the residence are affixed to the front of the residence. The mailbox for Apartment 1 is gold and has the number 1 prominently displayed.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

36. I have spoken with law enforcement personnel trained in computer evidence recovery who have knowledge about the operation of computer systems and the correct procedures for the seizure and analysis of computer systems.

37. These individuals have participated in the execution of numerous search warrants during which they have seized and/or examined computer systems. These individuals have also participated in several warrants that involved the search and/or seizure of, and has been responsible for analyzing, seized electronic data and records from those systems.

38. Based on my experience and training, plus the common sense knowledge that in today's technological world, computers and computer related media are used for communication and storage of data and information. As such, it is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format.

39. Furthermore, based upon my training, experience, and consultations with law enforcement personnel who specialize in searching computer systems, I have learned that searching and seizing information from computer systems and other storage media (including PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

40. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in mere desktop computers are capable of storing millions of pages of text; the storage capacity of other electronic devices (e.g. a micro drive, a thumb drive, etc.) can also be significant. Unlike the search of documentary files, computers store data in "files" that cannot easily be reviewed. For instance, a single 1 gigabyte of storage media is the electronic

equivalent of approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

41. The search through the computer (or other electronic media) itself is a time consuming process. Software and individual files can be "password protected." Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names ("Smith.ltr") can in fact be electronic commands to electronically cause the data to self-destruct. Also, files can be "deleted," but, unlike documents that are destroyed, the information and data from "deleted" electronic files usually remains on the storage device until it is "over written" by the computer. For example, the computer's hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non-deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the "pointers" have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the "deleted" file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time-consuming procedure to review the contents of the computer storage device so as to insure the integrity of the data and/or evidence. A single computer and related equipment could take many days to analyze properly.

42. Computer storage media are used to save copies of files and communications, and printers are used to make paper copies of these communications and files. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. All these parts of a computer are integrated into the entire operation of a computer. In order to evaluate the evidence most effectively, the computers and all of the related computer equipment described above should be available to a computer investigator/analyst.

43. Therefore, based upon my knowledge, training, and experience, as well as information related to me by Special Agents and others involved in forensic examination of computers, I am aware that searches for and seizures of evidence from computers commonly require Agents to seize most or all of a computer system's input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit.

44. Furthermore, searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

45. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

46. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

47. Based upon my training and experience and conversations with other law enforcement personnel, I am aware that a number of computer storage devices are quite small and portable, and can be easily hidden on a person. For instance, digital cameras can store numerous digital images on a disk approximately the size of a postage stamp. In addition, thumb drives, which are approximately the size of

a pocket knife, can hold numerous images and computer videos. I also know from my training and experience that these devices are often stored in vehicles to prevent other users in the home from discovering the existence of the child pornography collection. Your Affiant, therefore, also requests permission to search the person of Brock Likens for such evidence.

SEARCH METHODOLOGY TO BE EMPLOYED

48. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a) on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b) examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c) searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d) surveying various file directories and the individual files they contain;

e) opening files in order to determine their contents;

f) scanning storage areas;

g) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h) performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

49. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that someone using IP address 198.255.143.203, at a time it was assigned to the account subscribed to by Geri Hewitt, at the Subject Premises, is involved in the transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A, is located in the Subject Premises, on the person of Brock Likens, and within computers, computer equipment and/or other electronic media located therein.

50. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of (A) 11 Genesee Street, Apartment 1, Greene, NY 13778, (B) the person of Brock Likens and (C) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches, for the items listed in Attachment B.

Jenelle Corrine Bringuel
Special Agent
Federal Bureau of Investigation

Sworn to before me this 23rd day of January 2018.

HONORABLE ANDREW T. BAXTER
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A

PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) 11 Genesee Street, Apartment 1, Greene, NY 13778, (B) the person of Brock Likens and (C) any computers, computer equipment or computer storage media and other electronic or digital media capable of storing or transmitting digital data or digital media that are located during the course of said searches.

The apartment building of 11 Genesee Street, Greene, NY 13778, depicted below, is a two-story light grey home with a white front porch, situated on the south side of Genesee Street. The front exterior doors and trim around the windows are white. There are four grey steps leading up to the porch in the front of the residence. On the first level, the front doors are situated in the middle of the home, and there is a window situated to each side of the front doors. On the second level of the house, there are five windows across the front of the home. In what appears to be the attic of the residence, there is a window positioned on the front of the house, in the middle, directly above the front doors and a window on the second floor of the home. Apartment 1 is situated inside the left front door on the left side of the residence. The mailboxes for the residence are affixed to the front of the residence. The mailbox for Apartment 1 is gold and has the numbers 1 prominently displayed.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items of evidence in violation of Title 18 USC §§ 2252 and 2252A (transporting, distributing, receiving, or possessing child pornography):

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies);

any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, sd (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Computer and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored or maintained), books, notes, and reference materials.

10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.

11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.

12. Documents and records, in any form or format, regarding the identity of any person using P2P file sharing software and the use of any other methods of receiving, transporting, or distributing images of children engaged in sexually explicit conduct.

13. Documents and records regarding the ownership and/or possession of the searched premises.

14. Computer records and evidence identifying who the particular user was who received, downloaded, possessed, or accessed with intent to view any child pornography found on any computer or computer media (evidence of attribution), or who attempted to do any of the foregoing, and how the computer was used to effectuate that activity.

Materials Relating to Child Erotica and Depictions of Minors

15. Any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors.

16. Any and all chats, chat logs, emails, and other text documents, describing or relating to sexually explicit conduct with children, as well as fantasy writings regarding, describing, or showing a sexual interest in children.

17. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18 United States Code, Section 2256(2).

18. Any and all notebooks and any other records reflecting personal contact, and any other activities, with minors who may be visually depicted while engaged in sexually explicit conduct, or engaged in sexually explicit chat, email, or other communications.

19. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, notes, and sexual aids.

Photographs of Search

20. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.